

ABSTRACT

A quantum cryptographic device provides authentication services over the optical (quantum) channel [120] and the public channel [110] . In one implementation, polarizers [210, 215] generate optical pulses that have a polarization state based on a bit from a first bit sequence. A polarization rotator [220] further rotates the polarization basis of the optical pulse by a rotation angle specified by one or more bits of a second bit sequence. A receiving device receives the modulated optical pulses, demodulates the pulses, and may determine whether the optical channel can be authenticated. In an alternate implementation, phase modulation, instead of polarization modulation, is used to similarly modulate the optical pulses.